CLAIMS

1. Method for protecting the processing of sensitive information in a security module with a monolithic structure, the module comprising information processing means (31) and means for storing (32,33) information capable of being processed by said processing means, characterized in that it comprises the following steps:

- selecting a piece of sensitive information in the storage means;
- determining a specific condition for the integrity of said information;
- reading the information and transmitting it to the processing means;
- verifying during the processing of the information that the specific condition is satisfied;
- disabling the processing of the information if the specific condition is not satisfied.

2. Method according to claim 1, wherein the information is an operation code read in the storage means (32, 33), all of the operation codes being contained in a table having a content determined during the manufacture of the security module, and the specific integrity condition is the fact that the value of the information is equal to one of several set values.

3. Method according to claim 2, wherein the operation code to be processed is coded in the form of data bits and said bits do not all have the same binary value.

4. Method according to claim 1, wherein the specific integrity condition consists of checking a calculated piece of integrity data using the information read in the storage means (32, 33), the integrity data being calculated during the reading of the information and being transmitted to the processing means, the processing means calculating another piece of integrity data from the information received and checking for equality between the two integrity data.

5. Method according to claim 4, wherein the integrity data are calculated from at least one piece of calculation data whose value varies as a function of time.

6. Method according to claim 4, wherein the integrity data are calculated from at least one piece of calculation data whose value varies randomly.

7. Method according to claim 1, wherein the disabling of the processing of the information is performed by a microprogrammed instruction.

8. Method according to claim 7, wherein the microprogrammed instruction performs the following steps:

- writing a piece of disable data into a nonvolatile location of the storage means (32, 33);
- disabling the processing of the information.

9. Method according to claim 8 wherein, at the power-up of the module, a nonvolatile location of the storage means (32, 33) is read by the processing means (31), and the module is disabled if a value read at this location does not match.

10. Security module constituted by an electronic circuit with a monolithic structure and comprising information processing means (31) and information storage means (32, 33), the processing means selecting information extracted from the storage means in order to process it, characterized in that the processing means comprise means for verifying a specific integrity condition of a piece of sensitive information, and means for disabling the processing of the information, said disabling means being activated when the verification means have detected that the specific condition is not satisfied.

11. Security module according to claim 10, wherein the processing means (31) execute instructions corresponding to operation codes extracted from a table, characterized in that the table comprises a forbidden instruction value.

12. Security module according to claim 11, wherein the operation code to be processed is coded in the form of data bits, the security module comprising a means for reading the values of all the bits and a disabling means activated when the values of the bits are all identical.

13. Security module according to claim 10, wherein the processing means (31) execute instructions corresponding to operation codes extracted from a table, the security module comprising a means for reading an operation code and a disabling means activated during the reading of a forbidden operation code.

14. Security module according to claim 13, wherein the disabling means comprise a means for irreversibly writing an indicator into the storage means (32, 33), and a means for reading said indicator during the next power-up of the module.

15. Security module according to claim 10, comprising parity generators (7, 8) cooperating with the storage means, parity generators (11) cooperating with the processing means, and a comparator connected to each of the parity generators and capable of inducing an interrupt in the processing means.

16. Security module according to claim 15, wherein the operation of the parity generators (7, 8) varies as a function of time.

17. Security module according to claim 15, wherein the operation of the parity generators (7, 8) varies randomly.

18 Security module according to claim 14, characterized in that the irreversible writing of the indicator into the storage means (32, 33) is performed by executing a microprogrammed instruction.

19. Security module according to claim 10, characterized in that the security module is a microcircuit card.

Add A2